Issues and guiding principles for opening governmental judicial research data

Anneke Zuiderwijk[12], Marijn Janssen[1], Ronald Meijer[2], Sunil Choenni[23],
Yannis Charalabidis[4], Keith Jeffery[5]

[1] Delft University of Technology, Faculty of Technology, Policy and Management, Jaffalaan 5, 2628 BX Delft, The Netherlands, {a.m.g.zuiderwijk-vaneijk, m.f.w.h.a.janssen} @tudelft.nl
[2] Research and Documentation Center (WODC), Ministry of Security and Justice, Schedeldoekshaven 131, 2511 EM Den Haag, The Netherlands {r.f.meijer, r.choenni}@minvenj.nl
[3] Rotterdam University of Applied Sciences, Creating 010, G.J. de Jonghweg 4-6, 3015 GG, Rotterdam, The Netherlands, r.choenni@hr.nl
[4] University of Aegean, Department of Information and Communication Systems Engineering, Karlovassi, 83200 Samos, Greece, yannisx@aegean.gr
[5] Science and Technology Facilities Council, Rutherford Appleton Laboratory, Didcot, OX11 0QX, Harwell Oxford, United Kingdom, keith.jeffery@stfc.ac.uk

Abstract. The opening of data is considered to provide many benefits. However, opening up data by public bodies is a complex and ill-understood activity. Although many public bodies might be willing to open up their data, they lack any systematic guidance. In this paper, guidance is provided by investigating the publishing processes at the Dutch Research and Documentation Centre (WODC), which owns governmental judicial research data. We developed guidance by providing 1) a list of issues that play a role in deciding whether to open data, 2) an alternative to completely publishing data (i.e. restricted access) and 3) solutions for overcoming some of the issues. The latter include dealing with privacy-sensitive data, deletion policies, publishing after embargo periods instead of not publishing at all, adding related documents and adding information about the quality and completeness of datasets. The institutional context should be taken into account when using the guidance, as opening data requires considerable changes of organizations.

Keywords: open data, guiding opening data, institutional theory, opening governmental data, judicial research data.

1 Introduction

To quote from the Obama Administration, establishing openness in governmental organizations is considered to increase transparency, public participation and collaboration and therefore to "strengthen our democracy and promote efficiency and effectiveness in government" [1, p. 1]. Over the last years, various studies have argued that opening up data by governments may provide considerable advantages [2-

5]. The European Commission [6] states that "Public Sector Information is an important primary material for digital content products and services" [p. 1].

According to Geiger and Von Lucke [7], open governmental data can be defined as "all stored data of the public sector which could be made accessible by government in the public interest without any restrictions on usage and distribution" [p. 185]. We adopt this definition because it does not necessarily include the publication of all stored governmental data and it may exclude the publication of public sector data which must remain confidential or are privacy-sensitive.

Opening up data by data producers is a complex and ill-understood activity, because many barriers counteract these processes [8]. An important barriers is the threat of privacy violation by opening data and of being legally liable when opened data are misused [9]. Although many governmental organizations might be willing to open up their data, they lack guiding principles derived from practical case studies that help them in doing this [10]. Some helpful guidelines for opening up governmental data were published in the past [10, 11], but none of these guidelines were derived from and tested in practice.

The process of opening up public sector data demands considerable changes in the public sector, such as changes in the funding and reward systems of organizations. However, it is usually not possible to explain how those types of e-Government initiatives evolve over a certain period of time by the current e-Government linear progression models [12] and the development of composite e-Government services is usually ad-hoc [13]. Avgerou and Wahid propose to use institutional theory to study the implementation of information systems (IS) within organizations [14] and to explain how collective awareness or isomorphic change occurs [12, 15]. "Institutional theory postulates that organizations are driven to incorporate the prevailing rules, values, practices and logics in the institutional environment in order to increase their legitimacy and survival prospects" [16, p. 103, 17]. The latter may also be applied to governmental organizations that want to open up their data. In line with the foregoing, Scott [18] states that institutional theory "considers the processes by which structures, including schemas, rules, norms, and routines, become established as authoritative guidelines for social behavior" [p. 2]. From this perspective, Scott argues that "the boundaries of organizational fields are often vague or weak, allowing alternative logics to penetrate and support divergent models of behavior" [18, p. 11]. "Suppressed groups and interests may mobilize and successfully promote new models of structure and repertories of acting." [18, p. 11-12]. In line with this, Avgerou points out that "IS innovation is to a large extent sustainable by its own institutional forces, irrespective of its contribution to the processes of organizational change" [14, p. 1]. Moreover, from the perspective of institutional theory Orlikowski and Barley argue that IS-research should take into account the institutional context where IS are developed and implemented [19].Taking an institutional lens is considered to be useful for this research, as it shows that the current institutional context should be taken into account when focusing on organizational changes [19]. The aim of this paper is to develop guidance for opening up governmental data. We focus in particular on judicial research data and we use an institutional lens to understand the issues at hand [12, 14].

2 Research approach

The publishing process of datasets was investigated at the Research and Documentation Centre (Wetenschappelijk Onderzoek- en Documentatiecentrum; WODC) in the Netherlands. The WODC is a criminal justice knowledge center that is part of the Dutch Ministry of Security and Justice. In this organization data are mainly gathered to advise about and to define the current and future research agenda of the Dutch Ministry of Security and Justice, to answer policy-related questions and to indicate the possible implications of research findings for standing policy. For this purpose the WODC systematically collects, stores, enhances and provides criminal justice information produced by external organizations.

To get more insight in issues and guidance possibilities of the publishing process, we first thoroughly analysed 45 datasets of which 3 were opened and 42 were not opened. We inductively tried to identify issues that may be relevant for guidance for opening data. While doing this, the following aspects were taken into account:

  a. The context. For instance, the WODC works with confidential judicial research data, so that confidentiality and privacy-sensitivity should be taken into account.
  b. Current situations, including norms, values and beliefs [14, 18]. This means that the requirements and guiding principles should be embedded in the current situation, so that, for example, the limits of costs and time-consumption for an organization and the practices related to privacy sensitive information should be taken into account.
  c. Dominant rules, values, practices and logics in the institutional environment in order to increase their legitimacy and survival prospects [16, 17]. For instance, in the current practice of the WODC, data are not opened when the WODC wants to reuse the data in the future itself.
  d. The boundaries of organizational fields are often vague or weak, allowing alternative logics to penetrate and support divergent models of behavior. A new model of acting [18] that could be promoted at the WODC may be that certain types of descriptive, contextual and detailed metadata should be provided when data are published.

The previous steps resulted in an account of the issues that should be considered when opening governmental data. The list of issues was validated by carrying out eight interviews with three researchers working at the WODC. The validated account of the issues, the interviews and the aspects of institutional theory resulted in solutions for overcoming some of the issues. Finally, the possible solutions were discussed with two WODC-employees.

3 Case study background

The WODC aims to facilitate the reuse of research data, as this may provide the organization with benefits, such as the possibility to scrutinize and validate the data and to decrease the workload of the WODC. From 1982 until 2000 the WODC has opened up 21 datasets. In 2001, the Dutch Personal Data Protection Act (Wet

Bescherming Persoonsgegevens; WBP) was introduced, which aims to guarantee citizens the right to privacy protection [20]. In connection with this new act and an increase in attention for privacy protection in society, the WODC changed its open data policy in 2007. No WODC-datasets have been opened between 2000 and 2008.

Between 2008 and 2012, data that are considered by WODC-researchers to be qualified for public opening have partly been collected and stored in a so-called digital 'research data safe'. Over these 4 years, 45 datasets have been stored in the safe. Almost all the datasets contain crime-related research data that have been used to write reports on. The reports have been published between the years 2002 and 2009 and can be downloaded from www.wodc.nl. In 2008 and 2009, three WODC-datasets that were stored in the research data safe have been opened by means of publication by the Data Archiving and Networked Services (DANS, www.dans.knaw.nl).

In addition, the WODC receives individual requests for data (e.g. via e-mail). The WODC receives about 120 requests per year and most of them are being approved. The requests may be seen as a form of restricted access to data, since certain types of data users are excluded from access to certain data, such as students.

When we look at the WODC from an institutional perspective, we see that in line with the current norms WODC-data are usually not being opened. It was stated that the WODC considers opening up data to be risky when decisions about opening or not opening data are based only on random individual datasets, without taking a broader framework into account. It was also argued that the privacy act does not provide sufficient guiding principles for opening up data. Because of these risk avoiding norms, it becomes automatism not to open up the data and it becomes very difficult to change this culture. Therefore, we decided to develop guidance for opening up governmental data.

4 Guiding opening data

In section 4.1 guidance for opening data is provided in the form of a list of issues that should be taken into account when opening WODC-data. This list provides input for section 4.3, which presents ways in which these issues can be identified in organizations and by making a distinction between three ways of access.

4.1 Guidance by identifying issues for opening data

Institutional theory suggests to take into account current situations, including norms, values and beliefs when developing guiding principles for opening public sector data [19]. In the current situation, considerable issues play a role in determining whether to open data. In this section, guidance is developed in the form of a list enumerating the most important issues. In the list of issues a distinction was made between two categories: 1) general topics, which concern the dataset as a whole, and 2) dataset related issues, which concern the content of the dataset (see Table 1).

Table 1. List of issues that should be taken into account in developing guidance for opening up WODC-data.

Category	Issue
General	Policy confidentiality
	Deletion policy
	Embargo placement
	Organizational changes including time-consumption and changes in funding and reward systems
	Ownership
	Privacy-sensitivity and anonymization
	Lack of metadata
	(Re)use of data by WODC itself
	Policy-sensitivity
	Unlawfulness
Dataset	Completeness and exhaustiveness
	Representation
	Validity
	Reliability
	Clearness and comprehensiveness of column, row, value, variable and other names
	Provision of additional reports
	Overall data quality
	Other/rest category

In the first place policy confidentiality was considered to be an important issue. For instance, opening certain data may be dangerous to the state . Furthermore, the access to data may be restricted because a deletion policy may apply to the data [21] and/or they may be placed under an embargo period. Data can, for example, only be used for a year and should then be deleted in accordance with law or appointments that are made with data providers. When these data have been opened and should be deleted after a year, it is not possible to control whether all people that downloaded these data will also delete it. Other issues with regard to opening up data concern organizational changes. In this context, opening up data requires the creation of a policy for opening data and a focus on opportunities. With regard to individual datasets organizational changes concern changes in funding and reward systems and in time consumption structures [8]. In line with institutional theory, governmental organizations have a limited amount of money and time to spend on opening their data. In addition, data may be owned by different organizations so that the interests of all organizations should be taken into account [22].

Two very important aspects of opening governmental data are the right to privacy [3, 9] and the provision of metadata. In case that pending research is still using or will use certain datasets, it is not in the interest of the organization to open up these datasets. Besides, data may be policy sensitive. This issue is related to the unclearness of how data users are going to use open governmental data [8]. Policy sensitive data are not privacy sensitive data, but these data may be easily prone to misuse, misinterpretation and triggering of spurious findings. In addition to this, the consequences of publishing misused, minsterpretated and spurious findings may create negative publicity for the data producer. For example, the WODC monitors

crime statistics about business communities. Over the last year, the name of this monitor has become a brand name that is important for the WODC. Therefore, misuse of this brand name may result in negative publicity for the WODC. According to institutional theory, this institutional belief should be taken into account. Another issue that is important for the reputation of the organization and possible damage to the organization concerns the legal responsibility for opening data. Opening certain datasets may be unlawful. Multiple authors [3, 23, 24] state that organizations encounter substantial uncertainty, which is partly caused by legal principles competing with other values, such as security and system integration.
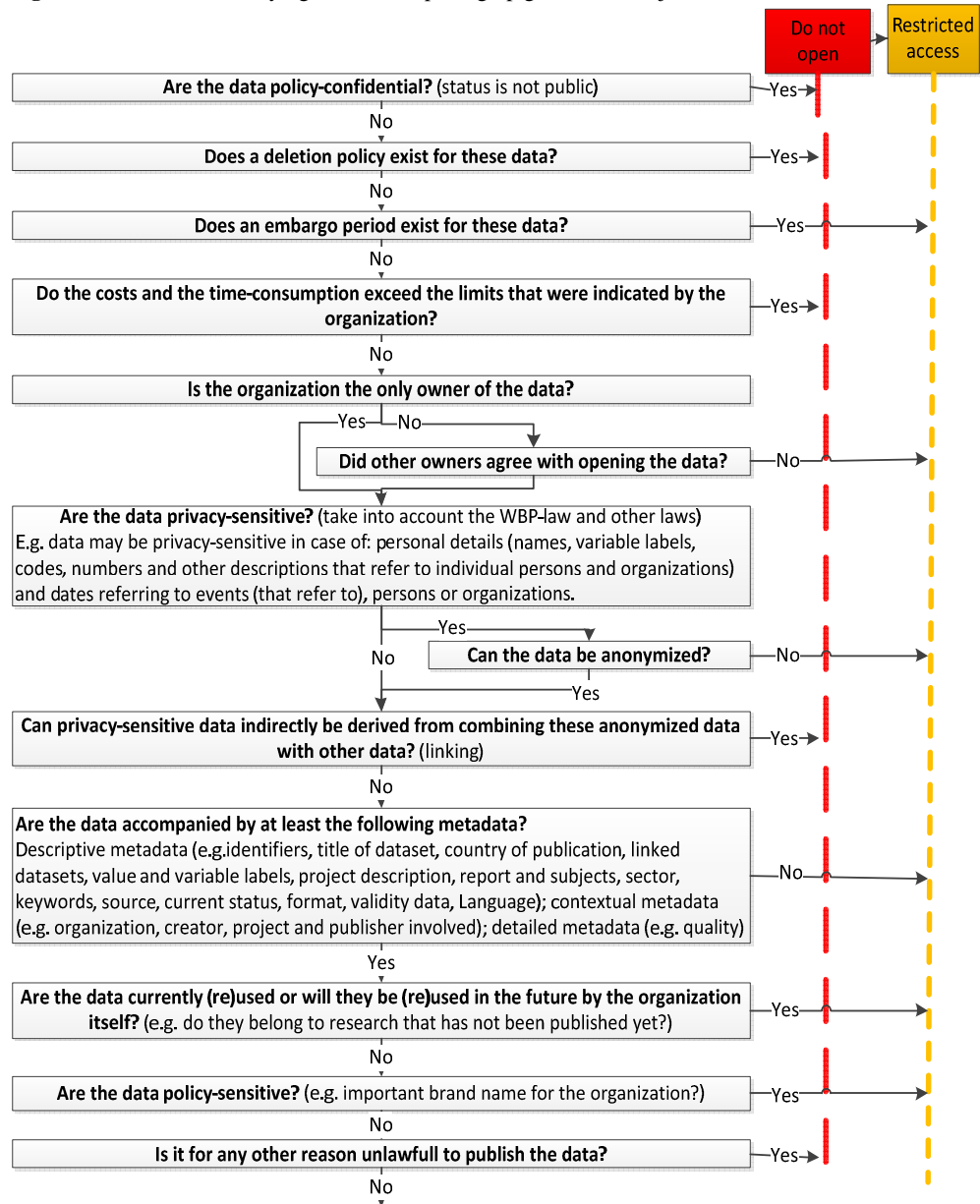
Other issues that are related to the context of the datasets concern completeness and exhaustiveness, the representation of the data, the validity, the reliability, the clearness and comprehensiveness and the provision of reports about analyses of the data. In line with these content related issues, the overall data quality should be taken into account. Finally, a remaining issue was added, as there may be other issues or combinations of issues that have not been identified by the analysis of datasets, but that would have been identified when other WODC-datasets or datasets of other organizations would have been analyzed.
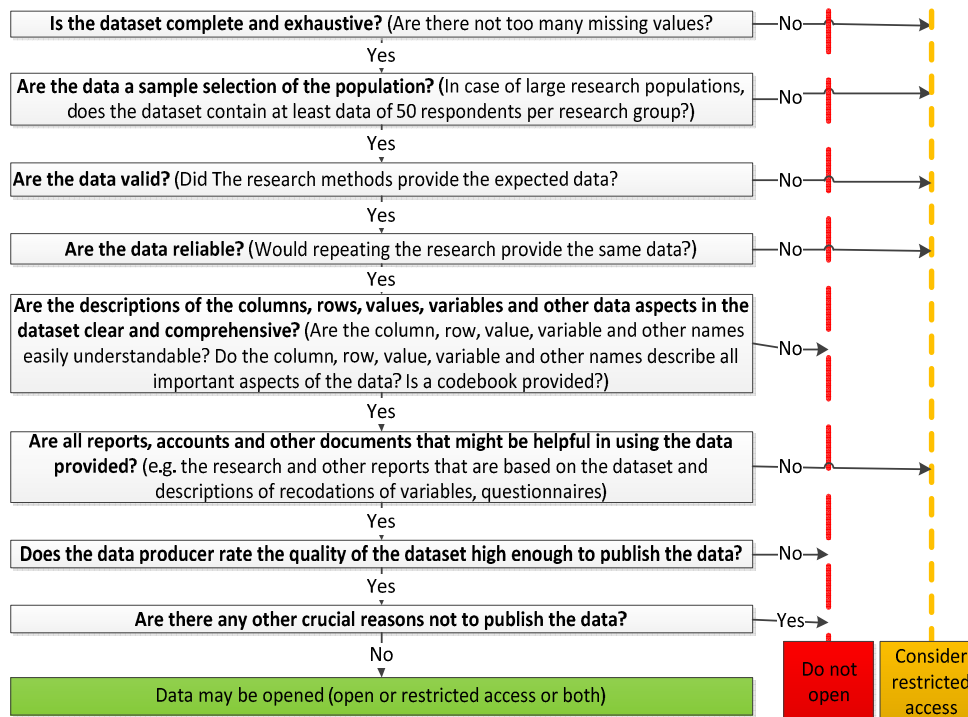
Issues that were identified frequently from the 45 datasets are privacy-sensitivity and anonymization, a lack of metadata, a lack of clearness and comprehensiveness of column, row, value, variable and other names and the overall data quality. Policy-sensitivity, deletion policy and unlawfulness were identified infrequently.

4.2 Guidance for the identification of issues

Figure 1 shows a systematic process for guiding the identification of all the issues that were enumerated in section 4.1. The questions that are expected to easily rule out opening up a certain dataset are placed on top of the list, whereas questions that require further examination are placed at the bottom of the list. This is done so that data that cannot be opened are quickly identified. Aspects of institutional theory were taken into account in Figure 1 by considering the risk avoiding governmental culture. For instance, due to the fear of wrongful interpretations of the data and the impact of wrongful interpretation on the organization, such as hitting the news with a damaged reputation, guidance is provided to make the chance on wrongful interpretations as small as possible. The latter is done by presenting a list of metadata aspects that should be provided together with the data themselves. Preferably, metadata would be derived directly from the source, although the interpretation of the data could still be difficult even with considerable metadata. Furthermore, the guidance takes into account the general legal framework that is already provided by the WBP, the Dutch Law for Openness of Administration (Wet Openbaarheid van Bestuur; WOB) and the general government conditions for distributing tasks for the performance of services (Algemene Rijksvoorwaarden voor het verstrekken van Opdrachten tot het verrichten van Diensten; ARVODI).

Fig. 1. Guidance for identifying issues for opening up governmental judicial research data.

Is the dataset complete and exhaustive? (Are there not too many missing values?)	—No
↓ Yes	
Are the data a sample selection of the population? (In case of large research populations, does the dataset contain at least data of 50 respondents per research group?)	—No
↓ Yes	
Are the data valid? (Did The research methods provide the expected data?	—No
↓ Yes	
Are the data reliable? (Would repeating the research provide the same data?)	—No
↓ Yes	
Are the descriptions of the columns, rows, values, variables and other data aspects in the dataset clear and comprehensive? (Are the column, row, value, variable and other names easily understandable? Do the column, row, value, variable and other names describe all important aspects of the data? Is a codebook provided?)	—No
↓ Yes	
Are all reports, accounts and other documents that might be helpful in using the data provided? (e.g. the research and other reports that are based on the dataset and descriptions of recodations of variables, questionnaires)	—No
↓ Yes	
Does the data producer rate the quality of the dataset high enough to publish the data?	—No
↓ Yes	
Are there any other crucial reasons not to publish the data?	—Yes
↓ No	
Data may be opened (open or restricted access or both)	

Do not open / **Consider restricted access**

4.3 Guidance for dealing with certain issues

In accordance with the possibilities that DANS provides for opening up data and the WBP, WOB and ARVODI, we suggest as guidance the use of three directions when opening WODC-data: open access, restricted access and combined open and restricted access. These directions will be explained in further detail in the following sections.

4.3.1 Open access

When all the questions in Figure 1 are answered and none of them points at the red 'do not open'-line, data can be opened according to the open access method. This means that data can be opened without any access restrictions.

A decrease of the risk on privacy violation while opening data in accord with open access could be arranged by anonymisation of personal details [e.g. see 25]. Also when the dataset is linked to other datasets, it should be avoided that this results in the exposition of the identity of individuals or groups of users [9, 25]. An example of the latter is provided by Kalidien et al. [9], who argue that the publication of data about the mean age of sex offenders per year, gender and city combined with data from other datasets, might expose the full identity of such a person [p. 3].

In addition, considerable attention should be paid to the provision of metadata, as metadata can yield significant benefits including creating order in datasets, improving

find ability, accessibility, storing and preservation of data, improving easily analyzing, comparing, reproducing, finding inconsistencies, assessing and ranking the quality of data and avoiding unnecessary duplication of data [26] and hereby encouraging linking open government data [27], so that public value can be created.

Moreover, attention should be paid to the representation (Do the data represent a sample selection of the population?), the validity (Did the research methods and definitions provide the researcher with the type of data that he/she wanted and expected to obtain?), the reliability (Would repeating the research provide the researcher with the same data as this research did?) and the clearness and comprehensiveness (Are the column, row, value, variable and other names easily understandable and do they describe all important aspects of the data?) of datasets. Furthermore, the provision of additional reports, accounts and other documents that are related to the dataset may be helpful in interpreting the data and these should therefore be published with the data and linked to them.

4.3.2 Restricted access

Under the circumstances that data cannot be opened by using the open access method, the data producer may consider opening up the data with restricted access. Data producers may, for example, fear opening postal codes on a street level or on a neighborhood level. Instead of not publishing the postal codes at all, these could be provided in accord with restricted access. We propose to consider restricted access when the questions in Figure 1 point at the orange 'restricted access'-line. When restricted access is provided, data users first have to ask the data producer for permission to obtain access to the dataset. The data producer may decide whether or not to provide access to the dataset, depending on the type of data, the type of user and the purpose of the use for these data, where the openness of data should be seen as a function with various parameters, such as:

- Retrievability of certain data. A dataset may contain personal details or show content restrictions and can therefore only be provided to the data user when he or she signs a contract with the data producer. Furthermore, certain datasets can be fragmented so that only by using a specific IT system it becomes possible to pull together the whole dataset. Similarly, it is possible to make data meaningless unless the end user (or the software the end-users is permitted to use) has a 'key' which transforms the data into something useable. Moreover, datasets may be put on a waiting list providing restricted access on the short term or opening the data after an embargo period.
- Accessibility of data for certain users. Access to data is usually arranged through software which makes it possible to restrict openness in line with the purpose of the data user, although no control exists on how data are used once the end-user has brought the data of interest outside of the IT system. However, one can restrict certain types of search, make some parts of the dataset invisible and restrict the use of the data in combination with other data.
- Purposes of certain data use. Data providers may only want to provide their data when they know for which purposes the data will be used. The data

provider may then have a better idea of the possible outcomes of the data use. Signing a contract is also a possible solution for this parameter.

- Users. Typically users may be classified in 'security rings' around a source; furthest out are all people, then increasingly restricted are continental nationals, country nationals, organizational employees (e.g. government), departmental employees, project or team employees, trusted employees. This may be more sophisticated by characterizing individual users according to previous history and other characteristics. Dependent on the type of user, the data producer may provide him or her with suitable specific advice with regard to this use.

4.3.3 Combining open and restricted access

Finally, a dataset may be opened with both the open access method as well as the restricted access method. Consider for example a dataset that consists of both privacy-sensitive data as well as non-privacy-sensitive data. The non-privacy-sensitive data may be opened with the open access method, whereas the privacy-sensitive data may be opened with the restricted access method. Whether a data producer wants to provide both open and restricted access depends on the considerations of the data producer.

5 Discussion and conclusions

From an institutional perspective, we found that on the basis of the prevailing standards, at the WODC-data are usually not opened. In the current situation risks are avoided as much as possible, due to the fear of privacy violations and the impact of inadequate decisions (violating privacy, hitting the news). However, the WODC has shown that it intends to open up more data by making policies and contracts about openness, such as a contract with a Dutch data archiving organization (DANS). Nevertheless, issues with privacy, legal liability, resource intensiveness, data quality and confidentiality are mentioned as considerable barriers for opening WODC-data. Because of these barriers only few datasets are opened.

Furthermore, institutional theory shows that organizations tend to have a risk averse culture and therefore views not-opening data as the default option. In addition, the opening up governmental data requires cultural changes in organizations.

An analysis of 45 datasets was performed of WODC-datasets that have and have not been opened in the past. The analysis resulted in a list of issues that should be taken into account when opening up a dataset. The general list of topics includes: confidentiality, deletion policies, embargo placement, cost and time consumption, ownership, privacy-sensitivity and anonymization, lack of metadata, reuse of data by the organization itself, policy-sensitivity and unlawfulness. Besides this general topic list, a list with content-related topics was created, which includes completeness and exhaustiveness, representation, validity, reliability , clearness and comprehensiveness of column, row, value, variable and other names, provision of additional reports, the

overall data quality and a rest category. On the basis of these issues, guidance for opening up governmental data was developed.

Because thinking binary in terms of opening and closing is too narrow, our guidance suggests alternative options to avoid rigorously not publishing data that potentially might be opened with three ways of opening up governmental data, namely open access, restricted access or combined open and restricted access. However, it may be difficult to simply follow the guiding principles by giving a yes/no-answer to the questions, because people have different values and they work in different institutional contexts and they may interpret the guidance differently. More insights in these institutional contexts and interpretations is necessary.

This research is a first effort in this field and the guiding principles that are presented in this paper are based on a single case. Further research should focus on the extension of the guiding principles and their applicability in other organizations. Furthermore, the guiding principles should be expanded, extended, specified and extensively tested. Nevertheless, the list of guiding principles can be used as a general means to check which issues should be discussed when one wants to open up governmental data.

References

1.	http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government
2.	European_Commission: Digital agenda: Turning government data into gold. (2011)
3.	Zhang, J., Dawes, S.S., Sarkis, J.: Exploring stakeholders' expectations of the benefits and barriers of e-government knowledge sharing. Journal of Enterprise Information Management 18 548-567 (2005)
4.	Charalabidis, Y., Ntanos, E., Lampathaki, F.: An architectural framework for open governmental data for researchers and citizens. In: Janssen, M., Macintosh, A., Scholl, J., Tambouris, E., Wimmer, M., Bruijn, H.d., Tan, Y.H. (eds.) Electronic government and electronic participation joint proceedings of ongoing research and projects of IFIP EGOV and ePart 2011, pp. 77-85, Delft (2011)
5.	Blakemore, M., Craglia, M.: Access to Public-Sector Information in Europe: Policy, rights and obligations. The Information Society 22, 13-24 (2006)
6.	http://ec.europa.eu/information_society/policy/psi/rules/eu/index_en.htm.
7.	Geiger, C.P., Lucke, J.v.: Open Government Data. Free accessible data of the public sector. In: Parycek, P., Kripp, M.J., Edelmann, N. (eds.) Conference for E-Democracy and Open Government (CeDEM11), pp. 183-194, Danube University Krems, Austria (2011)
8.	Boulton, G., Rawlins, M., Vallance, P., Walport, M.: Science as a public enterprise: the case for open data. The Lancet 377, 1633-1635 (2011)
9.	Kalidien, S., Choenni, R., Meijer, R.F.: Crime statistics online: potentials and challenges. In: Chun, S.A., Sandoval, R., Philpot, A. (eds.) Proceedings of the 11th Annual

International Digital Government Research Conference on Public Administration Online: Challenges and Opportunities, pp. 131-137. Digital Government Society of North America, Puebla, Mexico (2010)

10. Kalampokis, E., Tambouris, E., Tarabanis, K.: Open government data: A stage model. In: Marijn_Janssen_et_al (ed.) EGOV 2011, vol. 6846, pp. 235-246. LNCS, Delft, the Netherlands (2011)

11. Pollard, P.: Opening up government data: making the case. European Public Sector Information Platform (2011)

12. Wahid, F.: Explaining History of eGovernment Implementation in Developing Countries: An Analytical Framework. In: M._Janssen_et_al. (ed.) EGOV 2011, pp. 38–49. International Federation for Information Processing 2011, Delft (2011)

13. Lampathaki, F., Charalabidis, Y., Demetrios Sarantis, Koussouris, S., Askounis, D.: E-government services composition using multi-faceted metadata classification structures. Lecture Notes in Computer Science 4656, 116–126 (2007)

14. Avgerou, C.: IT and organizational change: an institutionalist perspective. Information Technology and People 13, 234–262 (2000)

15. Hassan, S., Gil-Garcia, J.R.: Institutional Theory and E-Government Research. In: Garson, G.D., Khosrow-Pour, M. (eds.) Handbook of Research on Public Information Technology, pp. 349-360. Information Science Reference, London (2008)

16. Phang, C.W., Kankanhalli, A., Ang, C.: Investigating Organizational Learning in eGovernment Projects: A Multi-Theoretic Approach. Journal of Strategic Information Systems 99–123 (2008)

17. Meyer, J.W., Rowan, B.: Institutionalized Organizations: Formal Structure as Myth and Ceremony. The American Journal of Sociology 83, 340-363 (1977)

18. Scott, W.R.: Institutional Theory: Contributing to a Theoretical Research Program. (2004)

19. Orlikowski, W.J., Barley, S.R.: Technology and institutions: what can research on information technology and research on organizations learn from each other? MIS Quarterly 25, 145-166 (2001)

20. Winter, H.B., Jong, P.O.d., Sibma, A., Visser, F.W., Herweijer, M., Klingenberg, A.M., Prakken, H.: Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk. Pro Facto, Rijksuniversiteit Groningen, De Jong Beleidsadvies, WODC, Groningen (2008)

21. Buruma, Y.: Het recht op vergetelheid. Politiële en justitiële gegevens in de digitale wereld. In: Broeders, D., Cuijpers, C., Prins, J.E.J. (eds.) De staat van informatie, WRR/AUP, nr. 25. Amsterdam University Press, Amsterdam (2011)

22. Faerman, S.R., McCaffrey, D.P., Slyke, D.M.V.: Understanding interorganizational cooperation: public-private collaboration in regulating financial market innovation. Organization Science 12, 372-388 (2001)

23. Edmiston, K.D.: State and local e-government: prospects and challenges. American Review of Public Administration 33, 20-45 (2003)

24. Dawes, S.S.: Interagency information sharing: Expected benefits, manageable risks. Journal of Policy Analysis and Management 15, 377-394 (1996)

25. Braak, S.v.d., Choenni, R., Meijer, R.F., Zuiderwijk, A.M.G.: Trusted third parties for secure and privacy-preserving data integration and sharing in the public sector. In: Luna-Reyes, L.F., Mellouli, S. (eds.) 13th Annual International Conference on Digital Government Research (dg.o 2012). ACM, University of Maryland, USA (2012)

26. Zuiderwijk, A.M.G., Jeffery, K.G., Janssen, M.F.W.H.A.: The necessity of metadata for open linked data and its contribution to policy analyses. In: Edelmann, P.P.N. (ed.) Conference on E-Democracy and Open Government (CeDEM12), pp. 281-294. Danube-University Krems, Krems, Austria (2012)

27. http://www.w3.org/TR/gov-data/